WiFi Networks

Chapter 8

Network & Security

Gildas Avoine

SUMMARY OF CHAPTER 8

- Wifi-based WLAN
- Authentication in WiFi Networks
- WEP Description
- Attacks on WEP
- WPA Motivations
- Architecture and Protocols
- Conclusion and Further Reading

WIFI-BASED WLAN

- Wifi-based WLAN
- Authentication in WiFi Networks
- WEP Description
- Attacks on WEP
- WPA Motivations
- Architecture and Protocols
- Conclusion and Further Reading

Eavesdropping

- Radio communications can be easily eavesdropped.
- Anyone with a radio interface can eavesdrop or inject traffic.
- Typical use inside: around 30 meters.

Source: Wikipedia

- Typical outdoor range with suited antenna: around 5 km.



Long Distance Records

- Line of sight required.
- 310 km by the Swedish Space Agency (ground – balloon).
- 382 km by EsLaRed of Venezuela (2007).

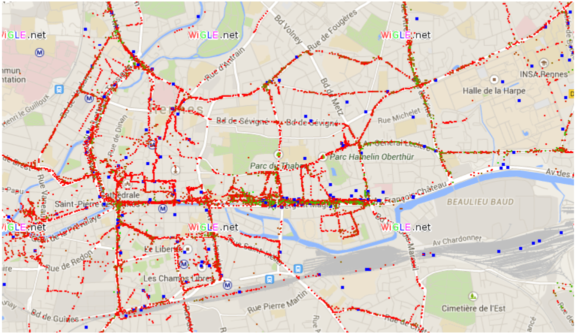
http://wndw.net/

http://wndw.net/

War Driving

- Discovering WiFi networks, no unauthorized access.
- Requirement: Laptop, 802.11 card, Software, GPS, Car.
- Listen and build maps of WiFi networks found while driving.
- Examples: `www.wigle.net` and `www.wardriving.com`.

Map of WiFi APs



Source: www.wigle.net

Security Needs

- Protecting a wireless network consists in ensuring:
  - Authentication.
  - Confidentiality.
  - Integrity.

AUTHENTICATION IN WIFI NETWORKS

Sol 1: Open Systems

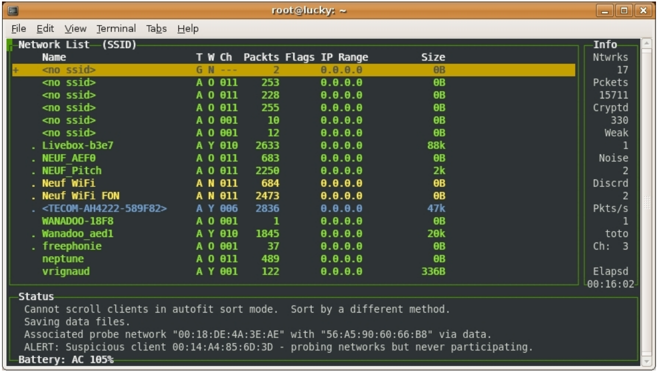
- No network authentication.
- Usually, providers impose authentication by default.
- Public free hot spots without network authentication.
- Non-free hot spots in hotels, train stations, etc.
- High-level authentication (eg. RADIUS Server).
- Communities sharing their access: FON (BT, Orange,...), etc.

Sol 2: Hidden SSID

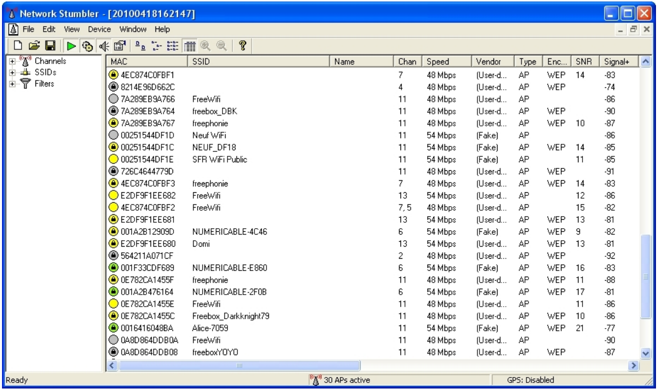
- Access points broadcast their SSID.
  - Allow clients to dynamically discover the AP.

- Can be used to authenticate a client.
  - Client must know the SSID.
  - Not secure because SSID can be eavesdropped.

Sniffing with Kismet (Linux)



Sniffing with Network Stumbler (Windows)

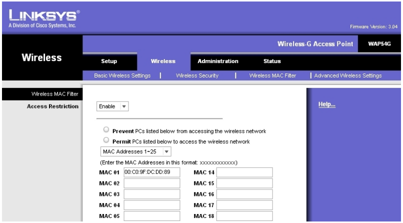


MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
4EC874C0FBF1			7	48 Mbps	(User-d...	AP	WEP	14	-83
8214E96D662C			4	48 Mbps	(User-d...	AP	WEP		-74
7A289EB9A766	FreeWifi		11	48 Mbps	(User-d...	AP			-86
7A289EB9A764	freebox_DBK		11	48 Mbps	(User-d...	AP	WEP		-90
7A289EB9A767	freephonie		11	48 Mbps	(User-d...	AP	WEP	10	-87
00251544DF1D	Neuf WiFi		11	54 Mbps	(Fake)	AP			-86
00251544DF1C	NEUF_DF18		11	54 Mbps	(Fake)	AP	WEP	14	-85
00251544DF1E	SFR WiFi Public		11	54 Mbps	(Fake)	AP		11	-85
726C4644779D			11	48 Mbps	(User-d...	AP	WEP		-91
4EC874C0FBF3	freephonie		7	48 Mbps	(User-d...	AP	WEP	14	-83
E2DF9F1EE682	FreeWifi		13	54 Mbps	(User-d...	AP		12	-86
4EC874C0FBF2	FreeWifi		7, 5	48 Mbps	(User-d...	AP		15	-82
E2DF9F1EE681			13	54 Mbps	(User-d...	AP	WEP	13	-81
001A2B12909D	NUMERICABLE-4C46		6	54 Mbps	(Fake)	AP	WEP	9	-82
E2DF9F1EE680	Domi		13	54 Mbps	(User-d...	AP	WEP	13	-81
564211A071CF			2	48 Mbps	(User-d...	AP	WEP		-92
001F33CDF689	NUMERICABLE-E860		6	54 Mbps	(Fake)	AP	WEP	16	-83
0E782CA1455F	freephonie		11	48 Mbps	(User-d...	AP	WEP	11	-88
001A2B476164	NUMERICABLE-2F0B		6	54 Mbps	(Fake)	AP	WEP	17	-81
0E782CA1455E	FreeWifi		11	48 Mbps	(User-d...	AP		11	-86
0E782CA1455C	Freebox_Darkknight79		11	48 Mbps	(User-d...	AP	WEP	10	-86
0016416048BA	Alice-7059		11	54 Mbps	(Fake)	AP	WEP	21	-77
0A8D864DDB0A	FreeWifi		11	48 Mbps	(User-d...	AP			-90
0A8D864DDB08	freeboxYOYO		11	48 Mbps	(User-d...	AP	WEP		-87

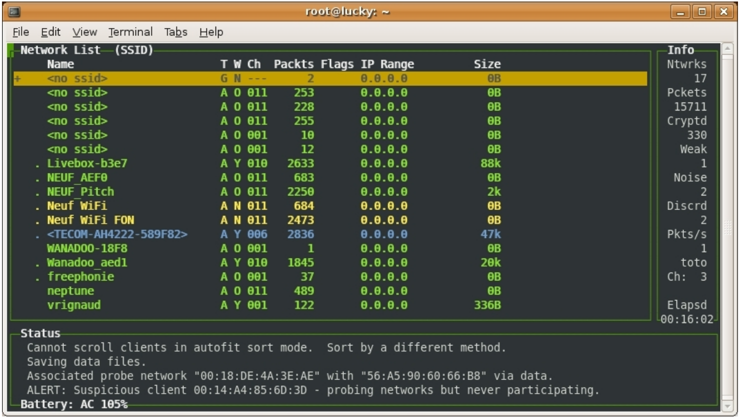
Sniffing with Inssider (Windows)

Sol 3: MAC Address Filtering

- The access point has a list of authorized MAC addresses.
  - The router checks the MAC address of the station trying to connect to the network.
  - The attacker can read the MAC address of a legitimate wireless station and replace his own MAC address with the stolen one.



Sniffing MAC Addresses



Modifying the MAC Address

```
ifconfig INTERFACE down
ifconfig INTERFACE hw ether NEW_MAC_ADR
ifconfig INTERFACE up
```

INFORMATIONS MODEM

Informations DHCP

Serveur	Adresse MAC	Adresse IP	Expiré dans
[redacted]	[redacted]	[redacted]	[redacted]
lucky	00:1C:BF:51:53:6F	192.168.1.3	6 jours, 19 heurres, 44 minutes, 27 secondes
[redacted]	[redacted]	[redacted]	[redacted]
lucky	00:1C:BF:51:53:6E	192.168.1.5	6 jours, 23 heurres, 53 minutes, 20 secondes

Sol 4: Crypto-based Authentication

- WEP.
  - Broken, should never be used.
- WPA.
  - Weak (urgent patch to WEP), should not be used.
- WPA2.
  - Secure (so far).
  - A dictionary attack can be performed.

WEP DESCRIPTION

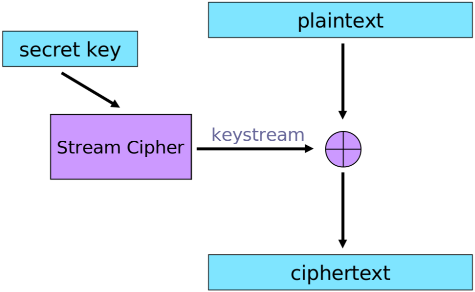
Generalities

- WEP = Wired Equivalent Privacy.
- Part of 802.11 Standard (1999).
- Goal of WEP is to make wireless LAN as secure as a wired LAN.

WEP Security Features

- No key management.
- No protection against replay attacks.
- Confidentiality (RC4 stream cipher encryption).
- Integrity (CRC-32 integrity mechanism).
- Authentication ("shared key" user authentication).

Confidentiality: Encryption using Stream Cipher



Stream Cipher RC4

- Designed by Ron Rivest (MIT) in 1987 for RSA Labs.
- Kept as a secret trade until 1994.
- Publicly disclosed in Sept. 1994 on Cypherpunks' mailing list.
- Bytes-oriented: Generate keystream byte at a step.
- Secret key of length from 1 to 256 bytes, usually 40 or 128 bits.
- Efficient, simple, elegant.

- Widely used:
    - Commercial softwares as MS Office, Oracle Secure SQL.
    - Network protocols as SSL, IPSec, WEP.
    - Copy protection: inside MS XBOX.

RC4 Steps

- KSA (Key-Scheduling Algorithm).
  - Initialization.
  - Scrambling ($N = 256$ rounds).
- PRGA (Pseudo-Random Generation Algorithm).

RC4 Steps

Initialization

For $i = 0$ To $N - 1$
Do $S_i = i$

Scrambling

$j = 0$
For $i = 0$ To $(N - 1)$
Do $j = (j + S_i + K_i) \bmod N$
Swap(S_i, S_j)
(K_i means $K_{(i \bmod L)}$ where $L = 16$)

Generation

Init: $i = j = 0$
$i = (i + 1) \bmod N$
$j = (j + S_i) \bmod N$
Swap(S_i, S_j)
Output $S_{(S_i + S_j)}$

RC4 Key $= K_0 \,||\, K_1 \,||\, K_2 \,||\, K_3 \,||\, K_4 \,||\, K_5 \,||\, \ldots \,||\, K_{N-1} \,||$

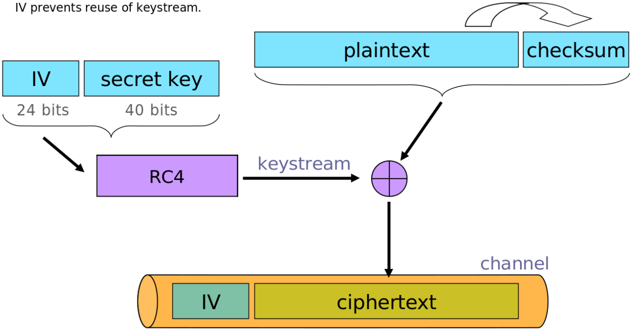
RC4 Key Example = 4 || 8 || 242 || 254 || ... ||

State Table S i	0	1	2	3	4	5	6	...	$N - 1$
Initialization	0	1	2	3	4	5	6	...	$N - 1$
$i = 0$, $j = 0 + S_0 + K_0 = 4$	4	1	2	3	0	5	6	...	$N - 1$
$i = 1$, $j = 4 + S_1 + K_1 = 13$	4	13	2	3	0	5	6	...	$N - 1$

Swap(S_1, S_{13})
Output S_{14}

RC4 for WEP Encryption

IV prevents reuse of keystream.



Danger if IV Reused

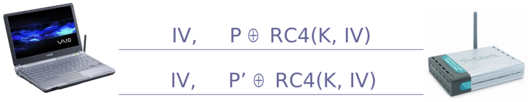
- WEP uses 24-bit (3 bytes) IV.
  - Each packet gets a new IV.
  - RC4 packet key: IV pre-pended to long-term key K.
- If K and IV are same, then same keystream is used.
- Problem: IVs frequently repeated.

IV Generation

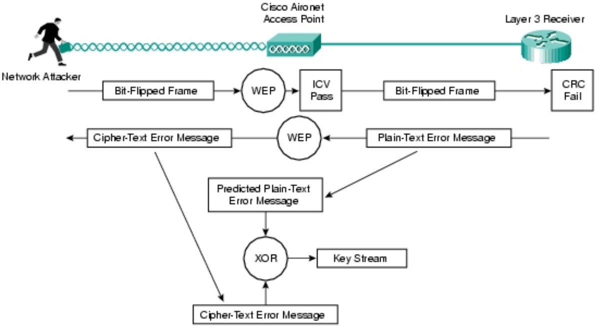
- The IV is often a counter that starts at zero.
  - Hence, rebooting causes IV reuse.
  - Also, there are only 16 million possible IVs, so after intercepting enough packets, they are almost sure to be repeated.
- There is a 50% chance of key-reuse after 2^{12} packets.
  - Birthday paradox.

Danger if IV Reused

- If IVs repeat, confidentiality is at risk.
- If two ciphertexts (C, C') use the same IV, then the xor of plaintexts leaks $(P \oplus P' = C \oplus C')$.
- If P is known, then P' is revelaed.



Getting Plaintext



WEP Integrity: CRC

- Integrity is ensured using a CRC.
- CRC does not provide a cryptographic integrity check.
  - CRC designed to detect random errors.
  - Not designed to detect intelligent changes.

CRC Property

- CRC is a linear function wrt to XOR.

$$CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$$

- Attacker observes $(M|CRC(M)) \oplus k$ where k is the keystream.
  - For any ΔM, the attacker can compute $CRC(\Delta M)$.
  - Hence, the attacker can compute:

$$\begin{aligned} & ([M|CRC(M)] \oplus K) \oplus [\Delta M|CRC(\Delta M)] \\ = \; & ([M \oplus \Delta M)|(CRC(M) \oplus CRC(\Delta M)]) \oplus K \\ = \; & [(M \oplus \Delta M)|CRC(M \oplus \Delta M)] \oplus K \end{aligned}$$

Example: ΔIP Address

- If the attacker knows destination IP address.
  - He can change IP address in the ciphertext.
  - And modify CRC so it is correct.
  - Then access point will decrypt and forward the packet to the attacker's selected IP address.
  - Requires no knowledge of the key K.

ATTACKS ON WEP

History Fact Sheet

- 1995 – Some security issues in RC4 (Weak keys). Roos, Wagner.
- 2001 - The insecurity of 802.11. Borisov, Goldberg, Wagner.
- 2001 - Weaknesses in the key scheduling algorithm of RC4: Fluhrer, Mantin, Shamir.
- 2002 - Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. Stubblefield, Ioannidis, Rubin.
- 2004 – Korek, improves on the above technique and reduces the complexity of WEP cracking. He proposed 17 attacks.
- 2005 – Klein introduces more correlations between the RC4 key stream and the key.
- 2007 – Tews, Weinmann, Pyshkin extend Korek's technique to further simplify WEP Cracking.
- 2013 – Sepehrdad,Vaudenay, Vuagnoux. Smashing WEP in a Passive Attack.

Weak Initialization Vectors

- Some IVs are weak, ie, they allow to guess some internal states, leading to the key.
- IV and first byte of plaintext and ciphertext must be known.
  - IV is sent in the clear.
  - Ciphertext is eavesdropped.
  - First bytes of ARP or TCP are fixed or can be easily guessed.

Requirements

- The 3-byte IV is sent in the clear (not secret).
- New IV sent with every packet.
- Long-term key K never changed.
- The key to encrypt a packet is $IV||K$.

Attack Assumptions

- Attacker knows IV $= K_0||K_1||K_2$.
- Attacker knows a ciphertext.
- Attacker knows the first bytes of the corresponding plaintext.
- The WEP long term key is denoted $K_3||K_4||K_5||\ldots$.
- The RC4 packet key is $K_0||K_1||K_2||K_3||K_4||K_5||\ldots$.

Fluhrer, Mantin, and Shamir's Attack

- The attacker observes the channel until he get a 3-byte IV of the form: IV $= (K_0, K_1, K_2) = (3, 255, X)$.
- Where X can be any arbitrary value.
- RC4 key for this packet is $3||255||X||K_3||K_4||K_5||\ldots$.

RC4 Steps with a Weak IV

Initialization

```
For i = 0 To N − 1
    Do S_i = i
```

Scrambling

```
j = 0
For i = 0 To (N − 1)
    Do j = (j + S_i + K_i) mod N
    Swap(S_i, S_j)
```

Generation

```
Init:  i = j = 0
i = (i + 1) mod N
j = (j + S_i) mod N
Swap(S_i, S_j)
Output S_(S_i+S_j)
```

RC4 Key $= K_0 \;||\; K_1 \;||\; K_2 \;||\; K_3 \;||\; K_4 \;||\; K_5 \;||\; \ldots \;||\; K_{N-1} \;||$

RC4 Key Example $= 3 \;||\; 255 \;||\; X \;||\; K_3 \;||\; K_4 \;||\; \ldots \;||$

State Table S i	0	1	2	3	4	...	$5+X$	...	$6+X+K_3$	...
Initialization	0	1	2	3	4	...	$5+X$	...	$6+X+K_3$	...
$i=0, j=0+S_0+K_0=0+0+3=3$	3	1	2	0	4	...	$5+X$	...	$6+X+K_3$	...
$i=1, j=3+S_1+K_1=3+1+255=3$	3	0	2	1	4	...	$5+X$	...	$6+X+K_3$	...
$i=2, j=3+S_2+K_2=3+2+X=5+X$	3	0	$5+X$	1	4	...	2	...	$6+X+K_3$	...
$i=3, j=(5+X)+1+K_3=6+X+K_3$	3	0	$5+X$	$6+X+K_3$	4	...	2	...	1	...

- Only 4 steps have been considered (there are actually 256 steps).
- Assume for now the initialization stops after $i = 3$.
- The outputted keystream is $S_{S_0+S_1} = S_3 = 6 + X + K_3$.
- So we have: KeyStreamByte $= 6 + X + K_3 \bmod N$.
- If KeyStreamByte is know, then $K_3 = (\text{KeyStreamByte} - 6 - X) \bmod N$.

Scrambling has 256 Steps

- Scrambling does not stop at i=3.
  - If S_0, S_1, and S_3 are not swapped in the remaining steps, the attack works.

- For the remaining initialization steps...
  - $i = 4, 5, 6, ...$ so index i will not affect values at indices 0,1 or 3.

- Assume index j is selected randomly:
  - At each step, probability is 253/256 that $j \notin 0, 1, 3$.
  - There are 252 steps after $i = 3$.
  - Probability that 0,1 and 3 not affected by j index after $i = 3$ step is $(253/256)^{252} \approx 0.0513$.

Recovering the next Key Bytes

- Can the attacker recover the full key?
- If he sees enough IVs he gets K_3.

- Suppose the attacker found K_3.
- Then how to find K_4?

- Consider IVs of the form: $\mathrm{IV} = (4, 255, X)$.
- After initialization step $i = 4$, one could show that: $\mathrm{keyStreamByte} = S4 = 10 + X + K_3 + K_4$.

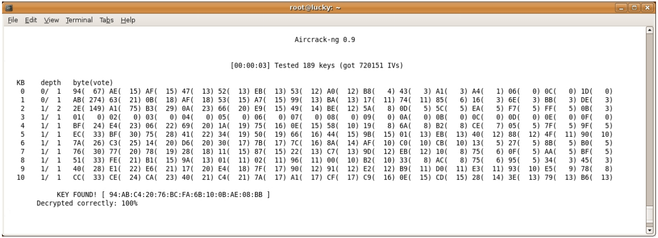
Fluhrer, Mantin, and Shamir's Attack

- 4 million IVs to recover a 128-bit key.
- Number of IVs linear with the key-length (vs exponential).
- Key is revealed byte after byte (sequentially).

Further Attacks

- Korek - 2004
  - Proposed 17 attacks based on FMS.
  - New classes of weak IVs.
  - 1 million IVs.
  - 2 bytes must be observable.
- Tews, Weinmann, Pyshkin (PTW) - 2007
  - Still new classes.
  - 80'000 IVs.
  - More bytes must be observable
  - Variant by Vaudenay/Vuagnoux 2007 (32'000 IVs)
  - Key bytes are no longer necessarily guessed sequentially.

- AirCrack-ng (http://www.aircrack-ng.org): implement Korek, PTW (needs ARP flooding).



WPA MOTIVATIONS

Introduction

- WPA: WiFi Protected Access.
- Goal is to replace WEP.
- WPA is a kind of urgent patch before the publication of 802.11i standard (WPA2).
- WiFi-compliant devices must implement WPA since 2003.
- WPA is designed such that old WiFi-compliant devices should be able to use WPA, possibly after a firmware update.

Features in Brief

- A counter is used to prevent replay attacks.
- The initialization vector is a 48-bit IV.
- User authentication while only device authentication in WEP.
- Keys are dynamically refreshed using TKIP.
- AES is used in WPA2 instead of RC4 in WEP and WPA.

- Two ways to use WPA: Personal and Enterprise.

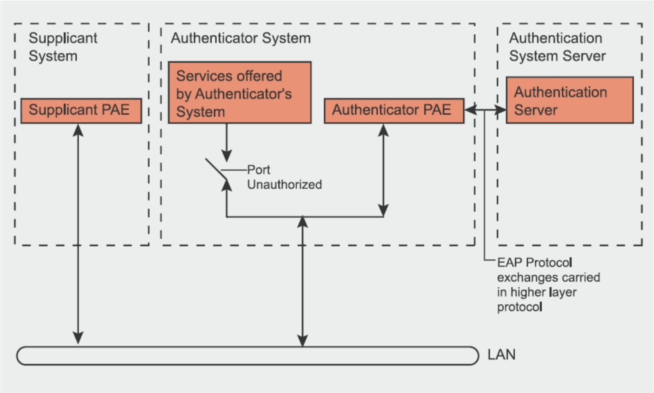
- Personal WPA utilizes pre-shared keys (PSK): every device connected to the AP uses the same passphrase.
  - Each user must enter a 256-bit key: 64 hex digits, or passphrase (8 to 63 printable ASCII characters) that is used to generate a key. The passphrase is hashed jointly with the SSID.
  - Authentication based on EAP-MD5 between the client and the Access Point.
  - Suited to home or small office infrastructure.

- Enterprise WPA uses an IEEE 802.1X Authentication Server that distributes different keys to the users.
  - Authentication of the user.
  - Requires an authentication server (eg Radius).
  - Centralizes management of user credentials.

ARCHITECTURE AND PROTOCOLS

- Supplicant: (party being authenticated).
- Authenticator (access point).
- Authentication Server.

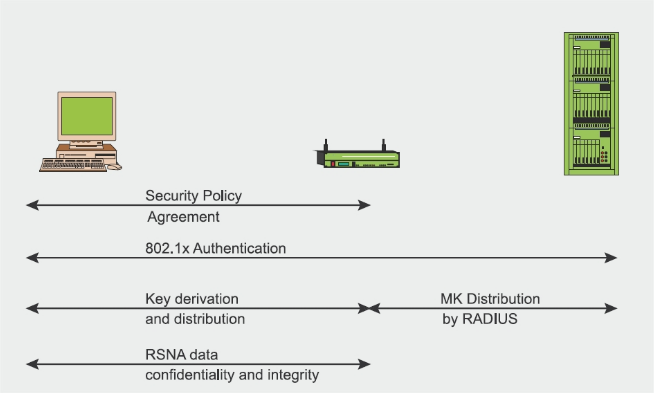
IEEE 802.1X Model from the IEEE 802.1X Spec.



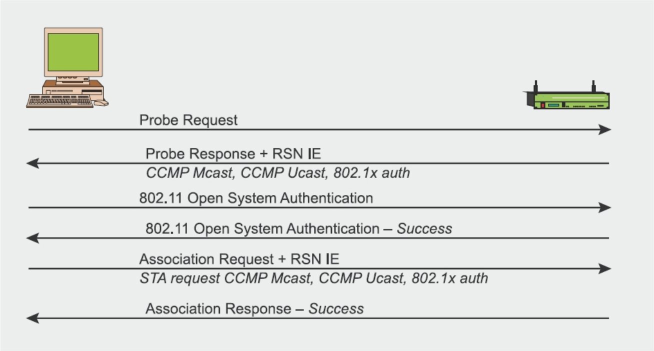
The pictures of this chapter are essentially from Wi-Fi security – WEP, WPA and WPA2 by Guillaume Lehembre, Hakin9, 2005.

- Agreement on the security policy.
- Authentication.
- Key derivation and distribution.
- Data confidentiality and integrity.

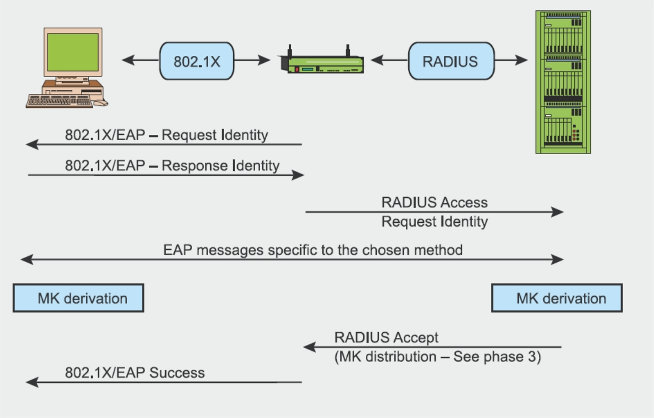
802.11i Operational Phases



Phase 1: Agreeing on the security policy



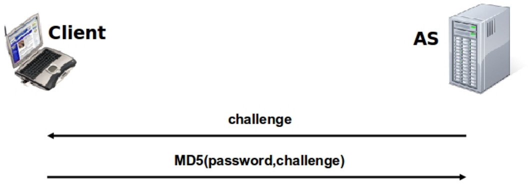
Phase 2: 802.1X Authentication



- EAP is a framework for transporting authentication protocols.
  - Not really an authentication protocol itself.
- Four types of packet: request, response, success and failure.
- Request packets are issued by the authenticator and solicit a response from the supplicant.
- Any number of request-response exchanges may be used to complete the authentication.
- A success (resp. failure) packet is sent to the supplicant if the authentication succeeded (resp. failed).

- Legacy based methods
  - EAP-MD5.
- Certificate based methods
  - EAP-TLS, EAP-TTLS, PEAP
- Password based methods
  - LEAP, SPEKE
- And many others...

- Authentication of the client only.
- MD5 message hashing algorithm.
- Very simple EAP method.
- It is not a secure EAP method.



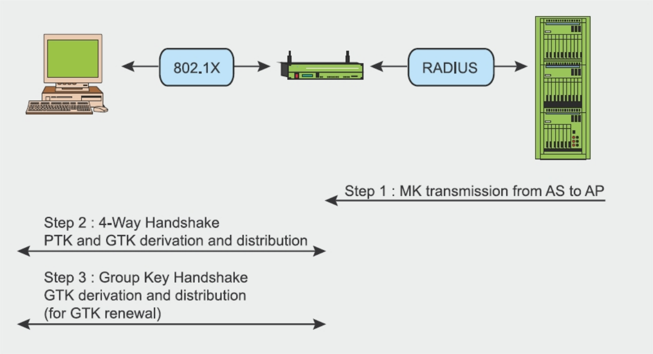
Phase 2: Extensible Authentication Protocol
EAP-TLS

- Mutual authentication and key exchange.
- Public key certificates (incl. the client).
- Strong authentication but requires PKI.

- Mutual authentication and key exchange.
- Public-key certificate (only the AP).
- A less secure authentication method can be used for the client (CHAP or PAP) through the secure channel.

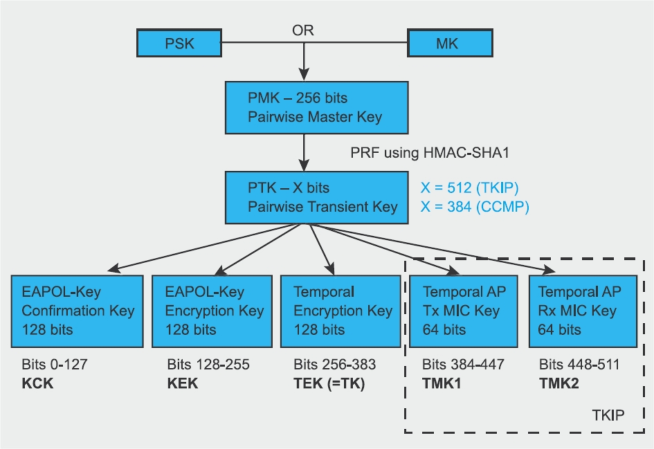
- PAP.
  - Upon reception of a request, the prover sends his password to the verifier.
- CHAP.
  - Upon reception of a challenge, the prover encrypts the challenge with his key and send the ciphertext to the verifier.

Phase 3: Key derivation and distribution



- MK: Master Key (= PSK when a preshared key is used).
- PMK: Pairwise-Master Key.
- PTK: Pairwise Transient Key (used for unicast).
- GTK: Group transcient key (used for multicast).

Phase 3: Pairwise Key Hierarchy



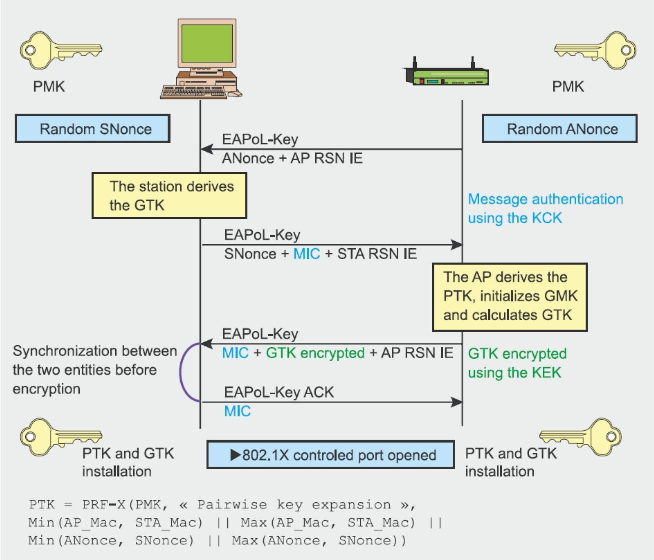
Phase 3: Pairwise Key Hierarchy

- KCK (Key Confirmation Key – 128 bits): Key for authenticating messages (MIC) during the 4-Way Handshake and Group Key Handshake.
- KEK (Key Encryption Key – 128 bits): Key for ensuring data confidentiality during the 4-Way Handshake and Group Key Handshake.
- TK (Temporary Key – 128 bits): Key for data encryption (used by TKIP or CMMP).
- TMK (Temporary MIC Key – 2x64 bits): Key for data authentication (used only by Michael with TKIP). A dedicated key is used for each side of the communication.

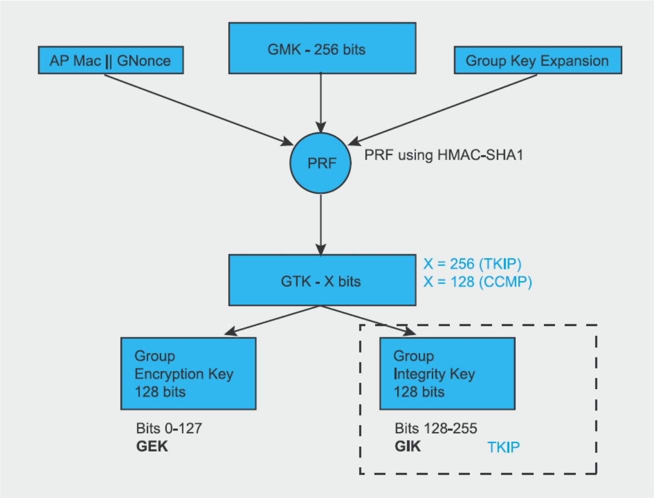
Phase 3: PMK

- PMK = PBKDF2(SSID, PSK).
- PBKDF2 is slow: 8192 runs of HMAC-SHA1.

Phase 3: 4-Way Handshake



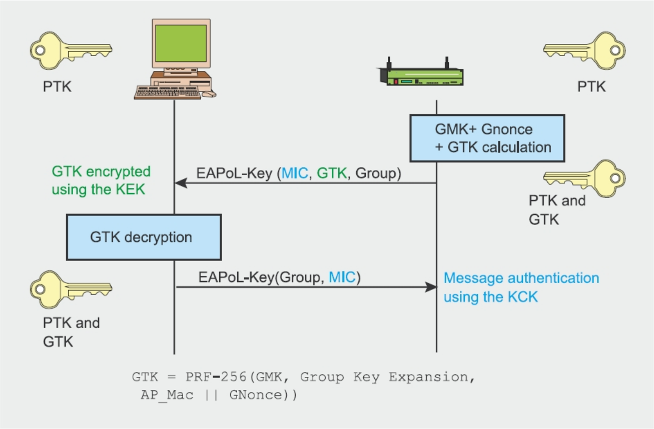
Phase 3: Group Key Hierarchy



Phase 3: Group Key Hierarchy

- GEK (Group Encryption Key): Key for data encryption (used by CCMP for authentication and encryption and by TKIP).
- GIK (Group Integrity Key): Key for data authentication (used only by Michael with TKIP).

Phase 3: Group Key Handshake

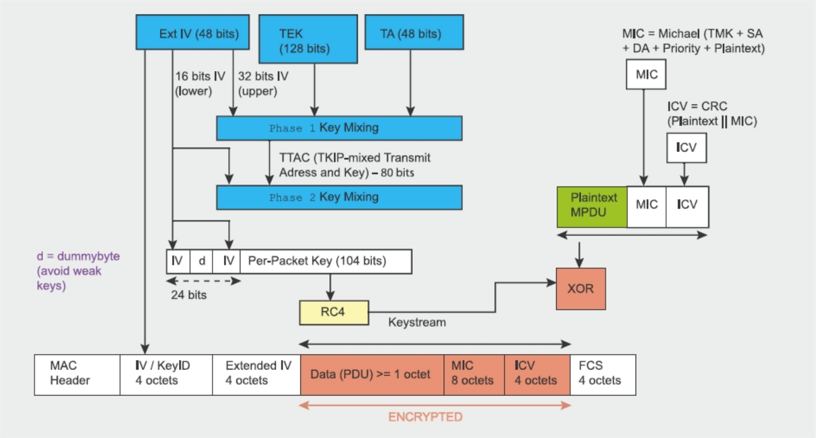


Phase 4: Data confidentiality and integrity.

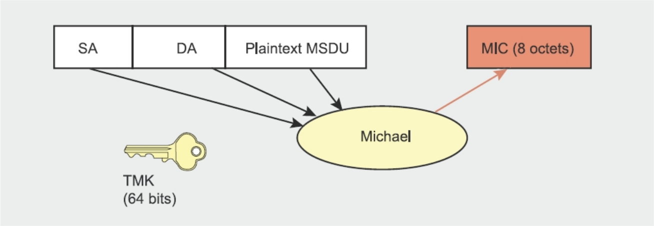
Two major suites of algorithms can be used with WPA:

- TKIP: RC4, MIC.
- CCMP: AES in Counter Mode (WPA2 only).

TKIP Key-Mixing Scheme and Encryption



MIC Computation using the Michael Algorithm

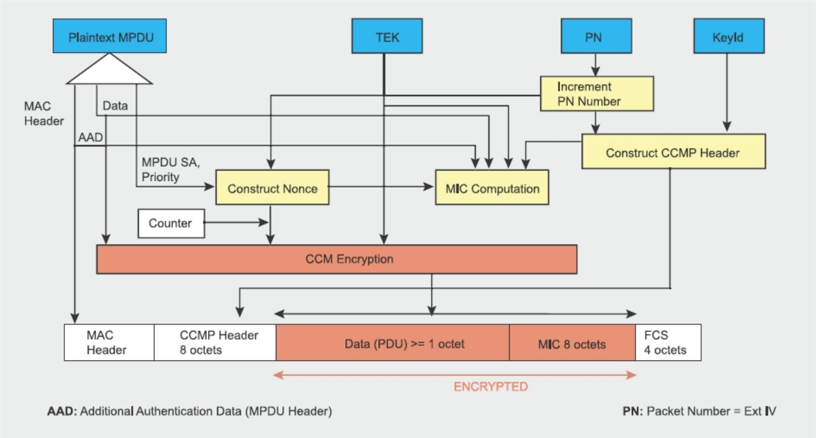


Michael MAC

A more secure Message Integrity Code (MIC)

- Michael algorithm instead of CRC32.
- Michael is keyed.
- Strongest MIC that was available with most older network cards.
- Due to weaknesses of Michael, the network is shut down during one minute if two frames fail to pass Michael check. Generation of new keys and reauthentication are required.

CCMP encryption



WPA2

- WPA2 implements the mandatory elements of 802.11i.
- WPA2 certification is mandatory for all new WiFi-compliant devices since 2006.
- AES-oriented, instead of RC4.

Attack on PSK

- All the keys derive from PSK.
- PMK = PBKDF2(SSID, PSK) then 4-way hanshake to derive the other keys.
- The handshake can be eavesdropped and used to check a candidate passphrase.
- Procedure.
  - For every candidate passphrase, compute the associated PMK.
  - Compute the PTK (4 HMAC-SHA1 computed on PMK and random values).
  - Compute the MIC (1 HMAC-SHA1 or MD5 and compare with the eavedropped one.
- To mitigate the problem, the SSID should not belong to the 1000 SSIDs as there exist precalculated tables for them.

Attack on TKIP

- Packet injection.
  - E.Tews and M.Beck (2008).
  - T.Ohigashi and M.Morii (2009).
  - F.Halvorsen, O.Haugen, M.Eian, S. Mjølsnes (2009).
  - 596 bytes within 18 min 25.
- Decryption of packets from AP to Client.
  - M.Beck (2010).

CONCLUSION AND FURTHER READING

WPA vs WPA 2

	WPA	WPA 2
Enterprise Mode	Authentication IEEE 802.1X/EAP Encryption TKIP/MIC	Authentication IEEE 802.1X/EAP Encryption AES-CCMP
Personal Mode	Authentication PSK Encryption TKIP/MIC	Authentication PSK Encryption AES-CCMP

Further Reading

- http://wiki-files.aircrack-ng.org/doc/tkip_master.pdf
- http://www.hsc.fr/ressources/articles/hakin9_wifi/